REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1, 4-6, 8-15, 17-20, and 22-25 are pending in the application. The Examiner additionally stated that claims 1, 4-6, 8-15, 17-20, and 22-25 are rejected. By this communication, claim 2 is cancelled and claims 1, 17, and 22 are amended. Hence, claims 1, 4-6, 8-15, 17-20, and 22-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-2, 4-6, 8, 13, 17-20, and 22-25 under 35 U.S.C. 103(a) as being unpatentable over Verbauwhede (US 20030202658), hereinafter, "Verbauwhede," in view of Wichman et al. (US 5884062), hereinafter, "Wichman." Applicant respectfully traverses the Examiner's rejections.

Claim 1 recites:

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

an x86-compatible microprocessor, comprising:

an instruction register within a x86-compatible microprocessor having a single, atomic cryptographic instruction disposed therein wherein said single, atomic cryptographic instruction prescribes that a user-generated key schedule be employed for execution of an encryption operation, and wherein said encryption operation that is prescribed by said single, atomic cryptographic instruction comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks;

a keygen unit, operatively coupled to said instruction register, configured to direct said x86-compatible microprocessor to load said user-generated key schedule; and

an execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said encryption operation, said execution unit comprising:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction; and

> an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said encryption operation, wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds.

Nowhere does the cited art disclose **a cryptography unit, . . . , an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said encryption operation**, as is recited in claim 1. Applicant has diligently searched the cited references to determine if there is any teaching, suggestion, or motivation to dispose a cryptography unit within an x86-compatible microprocessor along with the other noted parallel units, and to employ these units in parallel while executing an encryption operation. Applicant respectfully notes that the cited references utterly fail to teach the aforementioned limitation.

Nowhere does the cited art disclose **wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds**, as is recited in claim 1. Support for this limitation is found in several places in the specification. For example, see paragraph [0056]. Likewise, Applicant has diligently searched the cited references to find any disclosure or allusion whatsoever that would lead one skilled in the art towards the above-noted combination. Applicant reports that the cited references are completely silent in this regard.

Thus, for at least these reasons, it is respectfully submitted that the invention of claim 1 is patentably distinct and non-obvious in view of the cited art.

Claim 17 recites limitations similar to claim 1 with the exception that the single, atomic cryptographic instruction prescribes a decryption operation instead of an encryption operation.

Claim 22 recites substantially similar limitation as are recited in claim 1.

Accordingly, it is requested that the rejections of claim 1, 17, and 22 be withdrawn.

With respect to claims 4-6, 8, and 13 these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by the combination of the cited references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 4-6, 8, and 13.

With respect to claims 18-20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by the combination of the cited references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

Claims 23-25 depend from claim 22 and add further limitations that are neither anticipated nor made obvious by the combination of the cited references. Accordingly, Applicant respectfully submits that claims 23-25 are allowable as well and requests that the rejections be withdrawn.

The Examiner rejected claims 9-12 and 14-15 under 35 U.S.C. 103(a) as being unpatentable over Verbauwhede (US 20030202658 in view of Wichman et al. (US 5884062), in further view of Kessler et al. (US 6789147). Applicant respectfully traverses the Examiner's rejections and notes the claims 9-12 and 14-15 depend from claim 1, and add further limitations that are neither anticipated nor made obvious by the combination of the cited references. Accordingly, Applicant respectfully submits that claims 9-12 and 14-15 are allowable as well and requests that the rejections be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1, 4-6, 8-15, 17-20, and 22-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

10/22/2010

Date: _____